CLAIMS

1. Method for encrypting and decrypting a piece of information (I), said information (I) being represented by a string of symbols (S), said symbols (S) being included in a set of symbols hereinafter called the alphabet, said method being characterized in that it implements a pseudo-random generator (GA) that provides a sequence of values hereinafter called a random sequence (SA), the values forming said random sequence (SA) being included in a set hereinafter called the random value space;

said pseudo-random generator (GA) being able to be initialized, prior to utilization and the provision of said random sequence (SA), by means of a string of numbers hereinafter called the initialization key (CI), said initialization key (CI) determining the random sequence (SA) that will be provided by said pseudo-random generator (GA),

so that after a subsequent initialization using the same initialization key, the sequence of values provided will be the same as it was after the first initialization;

said pseudo-random generator also being characterized in that the knowledge of said sequence of values provided does not make it possible to discover said initialization key within a reasonable amount of time;

said method comprising three preliminary steps:

- the preliminary step of dividing said alphabet into two separate parts, one of said parts hereinafter being called the control alphabet and being composed of symbols designated not to be modified during encryption, the other of said parts hereinafter being called the message alphabet and being composed of symbols designated to be potentially modified during encryption,

so that each of the symbols used to represent the information is included in either said control alphabet or said message alphabet, there being no symbol common to these two alphabets,

- the preliminary step of defining a set, called the mask alphabet, formed of all or some of the elements in the random value space,

- the preliminary step of assigning a permutation of said message alphabet to each element of said mask alphabet;

said three preliminary steps being performed once and for all prior to the first implementation of said method;

the implementation of said method, in order to perform the operation of encrypting a piece of information (I) to be encrypted, comprising the following preliminary steps:

- the step of acquiring a string of numbers, hereinafter called the primary encryption key (CP),

- the step of constructing said initialization key (CI) from all or part of said primary encryption key (CP),

- the step of initializing said pseudo-random generator (GA) using said initialization key (CI);

said method consisting of selecting, one after another, the symbols (S) composing said information (I) to be encrypted, and of encrypting each of the symbols (S) thus selected by applying the following operations to it:

if said selected symbol (S) belongs to the control alphabet, it is not modified;

if said selected symbol (S) belongs to the message alphabet, the following steps are executed:

- the step of reading the next value in the random sequence (SA) provided by said pseudo-random generator (GA),

- if the value read in the preceding step is not an element of said mask alphabet, the step of reiterating the preceding step until an element of said mask alphabet is obtained,

the element of said mask alphabet determined in the preceding step will hereinafter be called the mask element (M),

- the step of selecting the permutation of the message alphabet assigned to the mask element (M) specified in the preceding step,

- the step of applying the permutation of the message alphabet selected in the preceding step to said selected symbol (S),

- the step of replacing said selected symbol (S) with the result (R) of the permutation performed in the preceding step;

these operations having been executed, the method moves on to the next symbol (S) in the information (I) to be encrypted, and so on, until all of the symbols in the information (I) to be encrypted have been processed.

2. Method according to claim 1, the implementation of said method, in order to perform the operation of decrypting a piece of information (I) to be decrypted, comprising the same preliminary steps as during the encryption,

so that the pseudo-random generator is initialized in the same way as during the encryption and therefore provides the same sequence of values as during the encryption;

said method consisting of selecting, one after another, the symbols (S) composing said information (I) to be decrypted, and of decrypting each of the symbols (S) thus selected by applying the following operations to it:

if said selected symbol (S) belongs to the control alphabet, it is not modified;

if said selected symbol (S) belongs to the message alphabet, the following steps are executed:

- the step of reading the next value in the random sequence (SA) provided by said pseudo-random generator (GA),

- if the value read in the preceding step is not an element of said mask alphabet, the step of reiterating the preceding step until an element of said mask alphabet is obtained,

the element of said mask alphabet determined in the preceding step will hereinafter be called the mask element (M),

- the step of selecting the inverse permutation of the permutation of the message alphabet assigned to said mask element (M) specified in the preceding step,

- the step of applying the inverse permutation selected in the preceding step to the selected symbol (S),

- the step of replacing the selected symbol (S) with the result (R) of the permutation performed in the preceding step;

these operations having been executed, the method moves on to the next symbol (S) in the information (I) to be decrypted, and so on, until all of the symbols in the information to be decrypted have been processed.

3. Method according to claim 1 or 2, the values in said random value space being numbers,

so that the mask alphabet is composed of numbers;

said method also including a preliminary operation for numbering the message alphabet, said numbering consisting of assigning to each symbol of the message alphabet, with no omission or repetition, a number between 0 and N-1, hereinafter called the number of the symbol, N representing the number of elements in the message alphabet, so that for any number between 0 and N-1, there is one and only one symbol of the message alphabet whose number is this number;

said method being characterized in that the result of the permutation of the message alphabet associated with a given mask element (M), for a given symbol (S) belonging to the message alphabet, can be calculated by successively executing the following steps:

- the step of determining the number of said given symbol (S),

- the step of adding said given mask element (M) to the number determined in the preceding step,

- the step of calculating the remainder of the division by N of the result of the addition performed in the preceding step,

- the step of determining the symbol of the message alphabet whose number is the number calculated in the preceding step; this symbol is the result (R) that was meant to be calculated,

hence, the permutation thus defined corresponds to a modulo-N addition on the symbol numbers, and the symbol determined in the preceding step is the result of this permutation applied to said given symbol.

4. Method according to claim 1 or 2, the values in said random value space being numbers,

so that the mask alphabet is composed of numbers;

said method also including a preliminary operation for numbering the message alphabet, said numbering consisting of assigning to each symbol of the message alphabet, with no omission or repetition, a number between 0 and N-1, hereinafter called the number of the symbol, N representing the number of elements in the message alphabet,

so that for any number between 0 and N-1, there is one and only one symbol whose number is this number;

said method being characterized in that the result of the permutation of the message alphabet associated with a given mask element (M), for a given symbol (S) belonging to the message alphabet, can be calculated by successively executing the following steps:

- the step of determining the number of said given symbol (S),

- the step of subtracting said given mask element (M) from the number determined in the preceding step,

- when the result of the subtraction performed in the preceding step is negative, the step of adding the number N to this result as many times as necessary to obtain a positive number,

- the step of calculating the remainder of the division by N of the result of the preceding step,

- the step of determining the symbol of the message alphabet whose number is the number calculated in the preceding step; this symbol is the result (R) that was meant to be calculated,

hence, the permutation thus defined corresponds to a modulo-N subtraction on the symbol numbers, and the symbol determined in the preceding step is the result of this permutation applied to said given symbol.

5. Method according to claim 1 or 2, the values in said random value space being numbers,

so that the mask alphabet is composed of numbers;

said method also including a preliminary operation for numbering the message alphabet, said numbering consisting of assigning to each symbol of the message alphabet, with no omission or repetition, a number between 0 and N-1, hereinafter called the number of the symbol, N representing the number of elements in the message alphabet,

so that for any number between 0 and N-1, there is one and only one symbol whose number is this number;

said mask alphabet including only non-zero numbers that are prime to N; said method being characterized in that the result of the permutation of the message alphabet associated with a given mask element (M), for a given symbol (S) belonging to the message alphabet, can be calculated by successively executing the following steps:

- the step of determining the number of said given symbol (S),

- the step of multiplying the number determined in the preceding step by the given mask element (M),

- the step of calculating the remainder of the division by N of the result of the multiplication performed in the preceding step,

- the step of determining the symbol of the message alphabet whose number is the number calculated in the preceding step. This symbol is the result (R) that was meant to be calculated,

hence, the permutation thus defined corresponds to a modulo-N multiplication on the symbol numbers, and the symbol determined in the preceding step is the result of this permutation applied to said given symbol.

6. Method according to claim 1 or 2, the values in said random value space being numbers,

so that the mask alphabet is composed of numbers;

said method also including a preliminary operation for numbering the message alphabet, said numbering consisting of assigning to each symbol of the message alphabet, with no omission or repetition, a number between 0 and N-1, hereinafter called the number of the symbol, N representing the number of elements in the message alphabet,

so that for any number between 0 and N-1, there is one and only one symbol whose number is this number;

said mask alphabet including only non-zero numbers that are prime to N; said method being characterized in that the result of the permutation of the message alphabet associated with a given mask element (M), for a given symbol (S) belonging to the message alphabet, can be calculated by successively executing the following steps:

- the step of determining the number of said given symbol (S),

- the step of determining a number which, when multiplied by the given mask element (M), differs from the number determined in the preceding step by a whole multiple of N,

- the step of calculating the remainder of the division by N of the number determined in the preceding step,

- the step of determining the symbol of the message alphabet whose number is the number calculated in the preceding step. This symbol is the result that was meant to be calculated,

hence, the permutation thus defined corresponds to a modulo-N division on the symbol numbers, and the symbol determined in the preceding step is the result of this permutation applied to said given symbol.

7. Method according to claim 1 or 2, the values in said random value space being numbers,

so that the mask alphabet is composed of numbers;

said method also including a preliminary operation for numbering the message alphabet, said numbering consisting of assigning to each symbol of the message alphabet, with no omission or repetition, a number between 0 and N-1, hereinafter called the number of the symbol, N representing the number of elements in the message alphabet,

so that for any number between 0 and N-1, there is one and only one symbol whose number is this number;

said mask alphabet including only non-zero numbers that are prime to Phi (N), where Phi (N) designates the number of integers between 1 and N-1 that are prime to N; said method being characterized in that the result of the permutation of the message alphabet associated with a given mask element (M), for a given symbol (S) belonging to the message alphabet, can be calculated by successively executing the following steps:

- the step of determining the number of said given symbol (S),
- the step of calculating the remainder of the division by N of the result of the raising of the number determined in the preceding step to a power equal to the given mask element (M),
- the step of determining the symbol of the message alphabet whose number is the number calculated in the preceding step. This symbol is the result (R) that was meant to be calculated,

hence, the permutation thus defined corresponds to a modular exponentiation on the symbol numbers, and the symbol determined in the preceding step is the result of this permutation applied to said given symbol.

8. Method according to claim 1 or 2, the values in said random value space being numbers,

so that the mask alphabet is composed of numbers;

said method also including a preliminary operation for numbering the message alphabet, said numbering consisting of assigning to each symbol of the message alphabet, with no omission or repetition, a number between 0 and N-1, hereinafter called the number of the symbol, N representing the number of elements in the message alphabet,

so that for any number between 0 and N-1, there is one and only one symbol whose number is this number;

said mask alphabet including only non-zero numbers that are prime to Phi (N), where Phi (N) designates the number of integers between 1 and N-1 that are prime to N; said method being characterized in that the result of the permutation of the message alphabet associated with a given mask element (M), for a given symbol (S) belonging to the message alphabet, can be calculated by successively executing the following steps:

- the step of determining the number of said given symbol (S),

- the step of determining a positive number which, when raised to a power equal to the given mask element (M), differs from the number determined in the preceding step by a whole multiple of N,

- the step of determining the remainder of the division by N of the number determined in the preceding step,

- the step of determining the symbol of the message alphabet whose number is the number calculated in the preceding step. This symbol is the result (R) that was meant to be calculated,

hence, the permutation thus defined corresponds to a root extraction in modular arithmetic on the symbol numbers, and the symbol determined in the preceding step is the result of this permutation applied to said given symbol.

9. Method according to claim 1 or 2, said method including a preliminary operation that consists of associating each element of the mask alphabet with a quadruplet of numbers noted p, q, r and s such that the number r and the result of the expression p.s-q.r are both non-zero numbers that are not multiples of N, N representing the number of elements in the message alphabet; said method also including a preliminary operation for numbering the message alphabet, said numbering consisting of assigning to each symbol of the message alphabet,. with no omission or repetition, a number between 0 and N-1, hereinafter called the number of the symbol,

so that for any number between 0 and N-1, there is one and only one symbol whose number is this number,

said method being characterized in that the result of the permutation of the message alphabet associated with a given mask element (M), for a given symbol (S) belonging to the message alphabet, can be calculated by successively executing the following steps:

- the step of determining the quadruplet of numbers p, q, r and s associated with the given mask element (M),

- the step of determining the number of the symbol (S) to be encrypted or decrypted, this number hereinafter being noted m,

- the step of calculating the expression m.r + s,

- the step, when the result of the calculation performed in the preceding step is zero or is a multiple of N, of calculating a number k such that the expression k.r - p is a multiple of N,

- the step, when the result of the calculation performed in the preceding step is neither zero nor a multiple of N, of calculating a positive number k such that the expression k.(m.r + s) – (m.p + q) is a multiple of N,

- the step of calculating the remainder of the division by N of the number k calculated in the preceding step,

- the step of determining the symbol of the mask alphabet whose number is the number calculated in the preceding step. This symbol is the result that was meant to be calculated,

hence, the permutation thus defined corresponds to the calculation of a homographic function in modular arithmetic on the symbol numbers, and the symbol determined in the preceding step is the result of this permutation applied to said given symbol.

10. Method according to any of claims 1 through 9, said method implementing a first pseudo-random generator (GA1) that can be initialized using the initialization key. (CI);

the values provided by said first pseudo-random generator being used as input data in a hash algorithm whose results are used to provide said random sequence (SA);

said pseudo-random generator (GA) consisting in the composition of said first pseudo-random generator (GA1) and said hash algorithm.

11. Method according to any of claims 1 through 9, said method also including the preliminary step of constructing, from all or part of said primary encryption key (CP), a string of numbers hereinafter called the secondary encryption key (CS);

said method implementing a first pseudo-random generator (GA1) that can be initialized using said initialization key (CI), the values provided by said first pseudo-random generator (GA1) being encrypted by means of a first encryption algorithm using the secondary encryption key (CS) as the encryption key, the results of said first encryption algorithm being used to provide said random sequence (SA);

said pseudo-random generator (GA) consisting in the composition of said first pseudo-random generator (GA1) and said first encryption algorithm.

12. System for encrypting and decrypting a piece of information (I), said information (I) being represented by a string of symbols (S), said symbols (S) being included in a set of symbols hereinafter called the alphabet; said alphabet being divided into two separate parts, one of said parts hereinafter being called the control alphabet and being composed of symbols designated not to be modified during encryption; the other of said parts hereinafter being called the message alphabet and being composed of symbols designated to be potentially modified during encryption;

said system being more particularly dedicated to securing communications between a computer, hereinafter called the client computer, and a network formed of one or more other computers, said system being interposed between said client computer and said network,

so that any information running between said client computer and said network that must be encrypted or decrypted passes through said system;

said system comprising a pseudo-random generator (GA) that provides a sequence of values, hereafter called a random sequence (SA), the values forming said random sequence (SA) being included in a set hereinafter called the random value space; some of these values being included in a subset of said random value space, a subset hereinafter called the mask alphabet;

said pseudo-random generator (GA) being able to be initialized, prior to utilization and the provision of said sequence of values, by means of a string of numbers hereinafter called the initialization key (CI); said initialization key (CI) determining the random sequence (SA) that will be provided by the generator;

said system also comprising:

- two input-output units (UES), one of which is dedicated to handling the communications between said system and said client computer, the other of which is dedicated to handling the communications between said system and said network;

- first processing means (TR1) that make it possible to acquire a string of numbers, hereinafter called the primary encryption key (CP), and to construct said initialization key (CI) from all or part of said primary encryption key (CP),

- second processing means (TR2) that make it possible to decide whether a value belonging to said random value space belongs to said mask alphabet,

- third processing means (TR3) that make it possible to read the successive values provided by said pseudo-random generator until an element (M) belonging to the mask alphabet is obtained,

- fourth processing means (TR4) that make it possible to decide which of the symbols (S) passing through said system are the symbols that must be encrypted or decrypted, and which are the symbols that must be transmitted without being modified,

- fifth processing means (TR5) that make it possible to select, from a given element of the mask alphabet hereinafter called the mask element (M), a permutation of the message alphabet, this permutation hereinafter being called the permutation assigned to the mask element (M), and that also make it possible, once the permutation assigned to the mask element (M) has been thus selected and a given element of the message alphabet (S) has been provided by one of said two input-output units, to determine the result (R) of this permutation applied to said given element (S) provided, and to send the result (R) thus determined to the other of said two input-output units.

13. System according to claim 12, said fifth processing means (TR5) also making it possible to select the inverse permutation of said permutation assigned to an element (M) of the mask alphabet.

14. System according to claim 12 or 13, the values in said random value space being numbers, said fifth processing means (TR5) also making it possible to associate a number with a symbol (S) of said message alphabet, to perform an addition in modular arithmetic between said number and an element (M) of said mask alphabet, and to associate the result of this addition with an element (R) of the message alphabet.

15. System according to claim 12 or 13, the values in said random value space being numbers, said fifth processing means (TR5) also making it possible to associate a number with a symbol (S) of said message alphabet, to perform a subtraction in modular arithmetic between said number and an element (M) of said mask alphabet, and to associate the result of this subtraction with an element (R) of the message alphabet.

16. System according to claim 12 or 13, the values in said random value space being numbers, said fifth processing means (TR5) also making it possible to associate a

number with a symbol (S) of said message alphabet, to perform a multiplication in modular arithmetic between said number and an element (M) of said mask alphabet, and to associate the result of this multiplication with an element (R) of the message alphabet.

17. System according to claim 12 or 13, the values in said random value space being numbers, said fifth processing means (TR5) also making it possible to associate a number with a symbol (S) of said message alphabet, to perform a division in modular arithmetic between said number and an element (M) of said mask alphabet, and to associate the result of this division with an element (R) of the message alphabet.

18. System according to claim 12 or 13, the values in said random value space being numbers, said fifth processing means (TR5) also making it possible to associate a number with a symbol (S) of said message alphabet, to perform an exponentiation in modular arithmetic of said number with an element (M) of said mask alphabet as the exponent, and to associate the result of this exponentiation with an element (R) of the message alphabet.

19. System according to claim 12 or 13, the values in said random value space being numbers, said fifth processing means (TR5) also making it possible to associate a number with a symbol (S) of said message alphabet, to perform a root extraction in modular arithmetic, and to associate the result of this root extraction with an element (R) of the message alphabet.

20. System according to claim 12 or 13, the number of symbols composing said message alphabet hereinafter being noted N, said system also including sixth processing means (TR6) that make it possible to associate an element (M) of said mask alphabet with a quadruplet of numbers noted p, q, r and s, said fifth processing means (TR5) also making it possible:

- to associate a symbol of said message alphabet with a number between 0 and N-1, this number hereinafter being noted m,
- to calculate the expression m.r + s,
- to determine whether an expression is zero or a multiple of N,
- to calculate a number k between 0 and N-1 such that the expression k.r – p is a multiple of N,

- to calculate a number k between 0 and N-1 such that the expression k.(m.r + s) – (m.p + q) is a multiple of N,

- to associate a number k thus calculated with an element (R) of the message alphabet.

21. System according to any of claims 12 through 20, said system including a first pseudo-random generator (GA1) that can be initialized using said initialization key (CI) and calculating means (H) that make it possible to apply a hash algorithm to the values provided by said first pseudo-random generator (GA1), the results of said hash algorithm being transmitted to said second and third processing means (TR2, TR3), said pseudo-random generator (GA) consisting in the combination of said first pseudo-random generator (GA1) and said calculating means (H) that make it possible to apply a hash algorithm to the values provided by said first pseudo-random generator (GA1).

22. System according to any of claims 12 through 20, said system including a first pseudo-random generator (GA1) that can be initialized using said initialization key (CI), said system also including seventh processing means (TR7) that make it possible to construct, from all or part of said primary encryption key (CP), a string of numbers hereinafter called the secondary encryption key (CS); said method also including calculating means (K) that make it possible to apply an encryption algorithm, using said secondary encryption key (CS) as the encryption key, said encryption algorithm being applied to the values provided by said first pseudo-random generator (GA1), the results of said encryption algorithm being transmitted to said second and third processing means (TR2, TR3), said pseudo-random generator (GA) consisting in the combination of said first pseudo-random generator (GA1) and said calculating means (K) that make it possible to apply an encryption algorithm to the values provided by said first pseudo-random generator (GA1).